53-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 164

RIN 0945-AA04

Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended

AGENCY: Office for Civil Rights, Office of the Secretary, Department of Health and Human Services.

ACTION: Request for Information.

SUMMARY: The Office for Civil Rights (OCR) at the United States Department of Health and Human Services (HHS or the Department) is issuing this Request for Information (RFI) to solicit public comment on certain provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, namely: The consideration of recognized security practices of covered entities and business associates when OCR makes determinations regarding fines, audits, and remedies to resolve potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule; and the distribution to harmed individuals of a percentage of civil money penalties (CMPs) or monetary settlements collected pursuant to the HITECH Act, which requires the Secretary of HHS (Secretary) to establish by regulation, and based upon recommendations from the Government Accountability Office (GAO), a methodology under which an individual who is harmed by an act that constitutes an offense under certain provisions of the HITECH Act or the Social Security Act relating to privacy or security may receive a percentage of any CMP or monetary settlement collected by OCR with respect to such offense.

DATES: Comments must be submitted on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Written comments may be submitted through any of the methods specified below. Please do not submit duplicate comments.

- *Federal eRulemaking Portal:* You may submit electronic comments at *https://www.regulations.gov* by searching for the Docket ID number HHS-OCR-0945-AA04. Follow the instructions for submitting electronic comments. Attachments should be in Microsoft Word or Portable Document Format (PDF).
- *Regular, Express, or Overnight Mail*: You may mail comments to U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HITECH Act Recognized Security Practices Request for Information, RIN 0945-AA04, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW, Washington, DC 20201.

All comments received by the methods and due date specified above may be posted without change to content to *https://www.regulations.gov*, which may include personal information provided about the commenter, and such posting may occur after the closing of the comment period. However, the Department may redact certain non-substantive content from comments before posting, including threats, hate speech, profanity, graphic images, or individually identifiable information about a third-party individual other than the commenter. In addition, comments or material designated as confidential or not to be disclosed to the public will not be accepted. Comments may be redacted or rejected as described above without notice to the commenter, and the Department will not consider in rulemaking any redacted or rejected content that would not be made available to the public as part of the administrative record. Commenters providing information regarding their organizations' implementation of recognized security practices should not include details that, if disclosed to the public, may put the security of the organizations' information systems at risk.

Because of the large number of public comments normally received on **Federal Register** documents, OCR is not able to provide individual acknowledgments of receipt.

Please allow sufficient time for mailed comments to be received timely in the event of delivery or security delays.

Please note that comments submitted by fax or email and those submitted after the comment period will not be accepted.

Docket: For complete access to background documents or posted comments, go to https://www.regulations.gov and search for Docket ID number HHS-OCR-0945-AA04.

FOR FURTHER INFORMATION CONTACT: Lester Coffer at (800) 368–1019 or (800) 537–7697 (TDD).

SUPPLEMENTARY INFORMATION:

OCR, which administers and enforces the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (HIPAA Rules), is issuing this RFI to improve its understanding of how covered entities and business associates (regulated entities) are voluntarily implementing recognized security practices as defined in Public Law 116-321, which added Section 13412 to the HITECH Act. The information received in public comments will help OCR determine what potential information or clarifications it needs to provide, through future guidance or rulemaking, to help regulated entities understand the application of the new law. This RFI also seeks public input on issues relating to the distribution of a percentage of CMPs or monetary settlements to individuals who are harmed by acts that constitute offenses under subtitle D of the HITECH Act or Section 1176 of the Social Security Act relating to privacy or security, as required by Section 13410(c)(3) of the HITECH Act. Among the issues on which OCR seeks public input are how to define compensable individual harm resulting from a violation of the HIPAA Rules and the appropriate distribution of payments to harmed individuals. OCR will use the information received in public comments to inform the development of future distribution methodology and policies.

I. Background

This RFI seeks public comment on how covered entities and business associates are voluntarily implementing recognized security practices as identified in Public Law 116-321,[1] and public input on potential information or clarifications OCR could provide on its implementation of the statute in future guidance or rulemaking. This RFI also seeks public comment on recommended methodologies for sharing CMPs or monetary settlements with harmed individuals as required by section 13410(c)(3) of the HITECH Act.[2]

A. Public Law 116-321 (Section 13412 of the HITECH Act, as amended)

Public Law 116-321, which adds section 13412 to Part 1 of subtitle D of the HITECH Act,[3] requires the Secretary to consider "recognized security practices" that HIPAA covered entities and business associates adequately demonstrate were in place for the previous 12 months when making determinations regarding fines (herein, "penalties") under section 1176 of the Social Security Act (as amended by section 13410 of the HITECH Act),[4] audits, and remedies to resolve potential violations of the HIPAA Security Rule[5] (Security Rule).[6] The statute does not expressly require rulemaking; however, the Department is seeking comment to inform potential future guidance or rulemaking that may help stakeholders better understand the application of the statute.

This RFI solicits comment on how covered entities and business associates understand and are implementing "recognized security practices," how they anticipate adequately

---

[1] *See* Section 1 of Pub. L. 116-321, 134 Stat. 5072 (January 5, 2021).
[2] The HITECH Act, enacted on February 17, 2009, as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. 111-5, modifies certain provisions of the Social Security Act pertaining to the HIPAA regulations, 45 CFR Parts 160 and 164.
[3] *See* 42 U.S.C. 17931 et seq.
[4] This RFI uses the terms "civil money penalty" or "penalty" in place of "fine" for consistency with section 1176 of the Social Security Act and the Enforcement Rule. *See generally* 42 U.S.C. 1320d-5 and 45 CFR Part 160, Subparts C, D, and E.
[5] 45 CFR Part 164, Subparts A and C. The HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information (ePHI) that is created, received, maintained, or transmitted by a regulated entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.
[6] Remedies agreed to by the covered entity or business associate and the Secretary generally consist of a signed resolution agreement that includes payment of a settlement amount, and a corrective action plan. *See* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html.

demonstrating that recognized security practices are in place, and other implementation issues they are considering or would like OCR to clarify for the public and stakeholders through potential guidance or rulemaking.

1. Recognized Security Practices

Public Law 116-321 defines "recognized security practices" as:

- the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology (NIST) Act;
- the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015; and
- other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.[7]

The statute does not require covered entities and business associates to implement recognized security practices,[8] nor does it provide criteria for covered entities or business associates to use when selecting which category of recognized security practices to implement (*i.e.*, developed under section 2(c)(15) of the NIST Act; promulgated under section 405(d) of the Cybersecurity Act of 2015; or other programs that address cybersecurity developed, recognized, or promulgated through regulations under other statutory authorities). However, the statute does require that recognized security practices must be consistent with Security Rule requirements.[9]

2. Adequately Demonstrate

Cybersecurity threats are a significant concern driving the need to safeguard electronic protected health information (ePHI) as required by the Security Rule. One of the primary goals of Public Law 116-321 is to encourage covered entities and business associates to do "everything

[7] *See* section 13412(b)(1) of the HITECH Act, 42 U.S.C. 17941(b)(1).
[8] *See* section 13412(b)(3) of the HITECH Act, 42 U.S.C. 17941(b)(3).
[9] *See* section 13412(b)(1) of the HITECH Act, 42 U.S.C. 17941(b)(1).

in their power to safeguard patient data."[10] To achieve this goal, Congress sought to "[incentivize] healthcare entities to adopt strong cybersecurity practices by encouraging the Secretary of HHS to consider entities' adoption of recognized cybersecurity practices when conducting audits or administering HIPAA fines."[11] Thus, the statute requires OCR to take into consideration in certain Security Rule enforcement and audit activities whether a covered entity or business associate has adequately demonstrated that recognized security practices were "in place" for the prior 12 months.

OCR believes that the phrase "had . . . [recognized security practices] in place," as used in Public Law 116-321,[12] is equivalent to the term "implement[ed]" as used and clarified in the Security Rule.[13] Therefore, it is insufficient for a regulated entity to merely establish and document the initial adoption of recognized security practices. For OCR to consider such practices when making determinations relating to penalties, audits, or other remedies, the entity must also demonstrate that the practices are fully implemented, meaning that the practices are actively and consistently in use by the covered entity or business associate over the relevant period of time.

3. The Previous 12 Months

The statute requires OCR, "when making determinations relating to fines under such section 1176 (as amended by section 13410) or such section 1177, decreasing the length and extent of an audit under section 13411, or remedies otherwise agreed to by the Secretary," to consider whether the covered entity or business associate has adequately demonstrated that the recognized security practices were in place for a period of "not less than

---

[10] Representative Pallone (NJ), "Requiring Secretary of Health and Human Services to Consider Certain Recognized Security Practices," Congressional Record 166:208 (December 9, 2020), p. H7089, available at https://www.congress.gov/congressional-record/2020/12/9/house-section/article/h7088-1.

[11] *Id.*

[12] *See* section 13412(a) of the HITECH Act, 42 U.S.C. 17941(a).

[13] "We use the term 'implement' to clarify that the procedures must be in use, and we believe that the requirement to implement policies and procedures requires, as an antecedent condition, the establishment or adaptation of those policies and procedures." Health Insurance Reform: Security Standards; Final Rule. 68 FR 8334, 8349 (February 20, 2003).

the previous 12 months." The statute does not state what action initiates the beginning of the 12-month look back period.

B. Section 13410(c)(3) of the HITECH Act

Section 13410(c)(1) of the HITECH Act[14] requires that any CMP or monetary settlement collected with respect to an offense punishable under subtitle D of the HITECH Act[15] or section 1176 of the Social Security Act,[16] insofar as such section relates to privacy or security, be transferred to OCR for the purpose of enforcing the provisions of subtitle D of the HITECH Act and subparts C and E of part 164 of title 45, Code of Federal Regulations.

Section 13410(c)(3) of the HITECH Act requires the Secretary to establish a methodology for the distribution of a percentage of a CMP or monetary settlement amount collected for noncompliance with the HIPAA Rules to an individual harmed by the noncompliance.[17]

Section 13410(d) of the HITECH Act modified section 1176(a)(1) of the Social Security Act to require that OCR base determinations of appropriate penalty amounts on the nature and extent of the violation and the nature and extent of the harm resulting from such violation.[18] The statute does not define "harm," nor does it provide direction to aid HHS in defining the term.

As part of its implementation of Section 13410(d) of the HITECH Act,[19] HHS amended the Enforcement Rule to identify four types of harm that OCR may consider as aggravating factors in assessing a covered entity's or business associate's CMP or proposed settlement amount: (1) physical harm, (2) financial harm, (3) reputational harm, and (4) harms that hinder one's ability to obtain health care.[20,21] In addition, HHS made clear in both the regulatory text

---

[14] *See* 42 U.S.C. 17939(c)(1).
[15] *See* 42 U.S.C. Chapter 156, Subchapter III.
[16] *See* 42 U.S.C. 1320d–5.
[17] *See* 42 U.S.C. 17939(c)(3).
[18] *See* 42 U.S.C. 17939(d).
[19] *See generally* 78 FR 5566 (January 25, 2013).
[20] 45 CFR 160.408(b).
[21] For further discussion of the factors considered by OCR when determining the amount of a CMP, including the types of harm, *see* 71 FR 8390, 8407-09 (February 16, 2006); 75 FR 40868, 40881 (July 14, 2010); and 78 FR 5585.

and preamble to the final rule that OCR is not limited to the four enumerated types of harm, stating that "in determining the nature and extent of harm involved, we may consider all relevant factors, not just those expressly included in the text of the regulation."[22]

This RFI solicits public comment on the types of harms that should be considered in the distribution of CMPs and monetary settlements to harmed individuals and the suitability of the described potential methodologies for sharing and distributing monies to harmed individuals, and invites the public to submit any alternative methodologies that are not identified herein. The discussion below informs commenters about OCR's enforcement of the HIPAA Rules, the challenges associated with defining harm to individuals, the potential distribution methodologies GAO recommended for consideration, and other implementation issues.

1. Background on OCR's Enforcement of the HIPAA Rules

OCR enforces the HIPAA Rules by investigating complaints submitted to OCR that allege noncompliance with the HIPAA Rules. OCR also conducts compliance reviews of potential noncompliance brought to OCR's attention by other means, such as through breach reports to the Secretary, to determine whether covered entities or business associates are in compliance with the HIPAA Rules.

OCR resolves the majority of HIPAA cases by providing technical assistance and/or obtaining voluntary corrective action by the covered entity or business associate. However, where the nature and scope of the noncompliance warrants additional enforcement action, OCR may pursue a resolution agreement and corrective action plan with a payment of a settlement, or it may impose a CMP.[23]

---

[22] 78 FR 5585.

[23] Information about previously imposed CMPs and resolution agreements entered into is available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

OCR is authorized under Section 13410 of the HITECH Act[24] to impose CMPs for violations occurring on or after February 18, 2009,[25] of:

- A minimum of $100 for each violation where the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
- A minimum of $1,000 for each violation due to reasonable cause and not to willful neglect, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $100,000. Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.
- A minimum of $10,000 for each violation due to willful neglect and corrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $250,000.
- A minimum of $50,000 for each violation due to willful neglect and uncorrected within 30 days, except that the total amount imposed on the covered entity or business associate for all violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

---

[24] 42 U.S.C. 1320d-5(a)(3).

[25] For violations occurring on or after November 3, 2015, the HITECH Act CMP amounts are adjusted annually pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvement Act of 2015. Sec. 701 of Public Law 114-74. The annual inflation amounts are found at 45 CFR 102.3.

The amount of a CMP that OCR pursues may vary based on the date and number of violations, the culpability of the entity, and the existence of certain mitigating and aggravating factors in accordance with 45 CFR 160.404, 160.406, and 160.408 and bounded by the calendar year caps stated above. For example, harm to an individual is an aggravating factor that may increase the CMP.[26] OCR may also determine that it is appropriate to waive a CMP in whole or in part to the extent the penalty would be excessive relative to the violation, in accordance with 45 CFR 160.412. In all cases, the total CMP may not exceed the statutory maximum established in the HITECH Act.[27]

When OCR's investigation indicates noncompliance with the HIPAA Rules, OCR may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means.[28,29] Informal means may include a settlement agreement, also called a resolution agreement (RA). RAs involve the payment of a monetary amount that is generally less than the maximum potential CMP for which the covered entity or business associate could be liable. They also generally include a corrective action plan that requires the covered entity or business associate to address remaining compliance issues and to undergo monitoring of its compliance with the HIPAA Rules for a specified period of time.

If the indicated noncompliance is not resolved by informal means, OCR so informs the covered entity or business associate and provides them an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under 45 CFR 160.408 and 160.410.[30] The covered entity or business associate must submit any such evidence within 30

---

[26] 45 CFR 160.408(b).
[27] *See* 45 CFR 160.404; *see also* 84 FR 18151 (April 30, 2019) for OCR's Notice of Enforcement Discretion Regarding HIPAA Civil Money Penalties for information on the annual limits to CMPs that may be imposed for HIPAA violations.
[28] 45 CFR 160.312(a)(1).
[29] OCR's website lists announcements of resolution agreements OCR has entered into with covered entities and business associates for alleged violations of the HIPAA Rules and CMPs OCR has imposed for violations of the HIPAA Rules. *See* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
[30] 45 CFR 160.312(a).

days of receipt of such notice. If OCR finds that a CMP should be imposed, the covered entity or business associate is informed of the finding in a Notice of Proposed Determination.

2. Determining Compensable Harm

As discussed above, the term "harm" is not defined by statute, and the HITECH Act does not provide HHS direction in how to define harm. Rather, the only qualification is that a relationship exists between the harm and the act of noncompliance with the HIPAA Rules. The Enforcement Rule identifies four types of harm as mitigating and aggravating factors that may be considered in determining the amount of CMPs – physical, financial, reputational, and ability to obtain health care – while leaving open the possibility of other types of harm.[31,32] However, the Enforcement Rule does not specifically define each of those types of harms, and the HITECH Act does not require OCR to apply those exact same harms to a methodology for distributing a percentage of CMPs and monetary settlements to harmed individuals. Therefore, OCR is considering what harms may make an individual eligible to receive such distributions.

3. Establishing a Methodology

Section 13410(c)(2) of the HITECH Act requires the Comptroller General to submit to the Secretary recommendations for a methodology under which an individual who is harmed by noncompliance with the privacy and security requirements related to PHI may receive a percentage of any CMP or monetary settlement collected by OCR. The HITECH Act directs HHS to establish a methodology for sharing CMPs and monetary settlements "based on the recommendations submitted" by the GAO.[33] The GAO recommendations do not address how to identify or define harm; instead, they offer distinct models for HHS to consider in developing its own methodology. [34]

---

[31] 45 CFR 160.408(b). ("The nature and extent of the harm resulting from the violation, consideration of which *may include but is not limited to* ….) (emphasis added).
[32] OCR is not required to prove that a violation of the HIPAA Rules has resulted in harm to individuals in order to determine that the imposition of a CMP is warranted. *See* 45 CFR 160.312 and 45 CFR part 160, subpart D.
[33] Section 13410(c)(3) of the HITECH Act, 42 U.S.C. 17939(c)(3).
[34] *See generally* Letter to HHS Secretary Kathleen Sebelius from GAO Acting General Counsel Lynn H. Gibson Recommending Models for the Distribution of Civil Monetary Penalties (August 9, 2010), available in the docket for this RFI.

In establishing a methodology, OCR must also consider the limitations on funding available for harmed individuals. Several factors influence OCR's assessment of this question. First, the HITECH Act does not guarantee or require that harmed individuals will be made whole by the sharing of CMPs and monetary settlements, nor does HIPAA provide a private right of action for an individual to sue a covered entity or business associate for violating their privacy rights. However, HIPAA does not preclude such remedies under state or other law.[35] Second, OCR is limited by statute in the total amount of a CMP that it can pursue for each alleged violation of the HIPAA Rules.[36] Finally, because OCR is not required to pursue an enforcement action to address every potential violation of the HIPAA Rules, every potential harm caused by such potential violations cannot necessarily be redressed.

GAO recommended three models for consideration: (1) individualized determination; (2) fixed recovery; and (3) hybrid. Below is a description of the potential models and examples that are in use today.

The Individualized Determination Model

The individualized determination model is based on the private civil action model whereby a plaintiff bears the burden of proof with respect to both the harm suffered by the plaintiff, including the nature and extent of the harm, and liability incurred by the defendant. Evidence concerning the nature and extent of harm supports the compensation awarded to a plaintiff. In civil actions, juries typically determine liability and compensation to be awarded based on instructions from the court regarding considerations when determining the award. In

---

[35] *See* 45 CFR 160.418. Further, every state's tort law system provides individuals a means for seeking redress when they are harmed by a negligent breach of duty. Such redress may include addressing potential harms caused by violations of federal or other privacy laws. Some states have also enacted a private right of action to allow individuals to recover when they are harmed by the impermissible sharing of their information. For instance, California Civil Code §§ 56 et seq. permits an individual whose medical information has been negligently disclosed to seek nominal damages of $1,000 without proving evidence of suffering. New York Public Health Law § 12 provides for civil penalties not to exceed $2,000 for violations of its health privacy law, and up to $10,000 for a violation directly resulting in serious physical harm to a patient. North Carolina allows an individual to bring a civil action for damages of up to $5,000 per incident or treble actual damages for each publication of personal information in violation of the state's identity theft law. North Carolina also provides an individual with a private right of action if the individual is harmed by an entity's failure to report the breach of personally identifiable information. *See* N.C. General Statute §§ 75-60 et seq, 75-16, 65-65.

[36] *See* section 13410(d) of the HITECH Act, 42 U.S.C. 17939(d).

general, "translating legally recognized harm into monetary awards is peculiarly a function of the jury," particularly when assigning value to intangible and noneconomic losses that may not be readily quantified, such as pain and suffering, loss of reputation, or emotional distress.[37]

A variation of the individual approach is the civil action known as a class action, where a group of similarly harmed individuals may pursue claims for redress of harm together. Class actions occur for several reasons, such as for judicial economy to avoid multiple adjudications of the same legal or factual issues or to permit a group to pursue recovery when it may not be economically feasible to pursue claims as individuals. While the burdens of proof for harm and liability that exist for a private civil action remain the same for plaintiffs, awards are shared among the class of harmed individuals, often based on a fixed percentage of the total recovery amount.

The Consumer Financial Protection Bureau (CFPB or the Bureau) uses an individual assessment model to distribute monetary awards for economic harms. The CFPB has authority for oversight and regulation of consumer financial products and services, including the ability to direct money into the Consumer Financial Civil Penalty (CFCP) Fund, which may then be used to compensate individuals (referred to in regulation as "victims") who have been harmed by an activity for which a penalty was imposed by the Bureau.[38] The CFCP Fund's rules define compensable harm for a victim as: 1) the victim's share of an ordered redress[39] amount; 2) if no ordered redress amount, then a harm formulation contained in the underlying final order (if any); or 3) if no ordered redress or harm formulation, then the victim's out of pocket losses, except to the extent such losses are impracticable to determine.[40] Payments from the Fund may only be

---

[37] *See* GAO Letter, *supra* note 34, at 4.

[38] *See* Wall Street Reform and Consumer Protection Act § 1017(d)(2) (Pub. L. 111-203), rules finalized at 12 CFR Part 1075.

[39] Redress is defined as "any amounts – including but not limited to restitution, refunds, and damages – that a final order requires a defendant:

(1) To distribute, credit, or otherwise pay to those harmed by a violation; or
(2) To pay to the Bureau or another intermediary for distribution to those harmed by the violation." *See* 12 CFR 1075.101."

[40] 12 CFR 1075.104(c).

made to eligible victims for compensable harm when calculable and only to the extent a person has not received or is not reasonably likely to receive full compensation for the same compensable harm from another source.[41]

Compensation from the CFCP Fund occurs in a two-step process. First, the Fund administrator allocates funds for payment to eligible victims. Second, the Fund administrator designates a payments administrator with responsibility for distribution of funds; the distribution methodology is not detailed in the CFPB's regulations.[42] Funds received by the CFPB for a given violation are available for distribution to any eligible class of victims with uncompensated harm where distribution is practicable. To the extent that funds remain after all eligible victims have been fully compensated, CFCP Fund amounts not used for individual compensation may be used by the CFPB for consumer education and financial literacy programs.

The Fixed Recovery Model

Under the fixed recovery model, awards are generally either fixed or calculated by a formula established by law, and recovery is based on the prescribed formula. The GAO cites the Black Lung Benefits Act[43] (BLBA) as one example. The BLBA provides benefits to coal miners and their families for disability or death due to pneumoconiosis (also known as black lung disease) resulting from employment in and around coal mines. To receive an award, an individual or family must first provide medical information demonstrating the medical condition, similar to the evidence of harm required in the individualized determination model. Recovery is based upon a statutory formula and reduced when compensation for the same condition is received from other sources (*e.g.,* worker's compensation for pneumoconiosis). An individual's

---

[41] 12 CFR 1075.104(b).

[42] 12 CFR 1075.108(b) requires the payments administrator to "submit to the Fund Administrator a proposed plan for the distribution of funds allocated to a class of victims," while 12 CFR1075.108(c) details the contents the Fund Administrator may require the payments administrator to include. Thus, the distribution methodology is determined on a case-by-case basis. According to the CFPB website, "Some payments are administered by the defendant….In other cases, we may require the person or company that violated the law to make the payment to the CFPB, and then we distribute that money to the victims." https://www.consumerfinance.gov/enforcement/payments-harmed-consumers/payments-by-case/. A full listing of redress payments administered by the Bureau and victim payments from the CFCP Fund is available at the website above.

[43] Pub. L. 92-303, 30 U.S.C. Chapter 22, Subchapter IV.

recovery does not vary due to the specific individual's economic or noneconomic harm as in the individualized determination model, but the fixed determination model does offer advantages in its relative ease of administration.

The Hybrid Model

The hybrid model combines elements of the individualized determination and fixed recovery models. GAO notes that hybrid models may be used to reflect uncertainty regarding the types of harm that can be demonstrated with evidence. For example, the Privacy Act of 1974 permits a private right of action for the unlawful disclosure of an individual's records by a federal agency. A plaintiff who demonstrates that a federal agency unlawfully disclosed the plaintiff's records in a willful or intentional manner may receive the minimum amount of $1,000 when the evidence of quantifiable harm is less than $1,000 and may recover the full amount of actual damages when there is evidence of quantifiable harm exceeding $1,000. In a 2009 class action settlement by the Department of Veterans Affairs involving Privacy Act violations, the VA payments were limited to a minimum of $75 and maximum of $1,500.[44] When settling a case with ChoicePoint[45] under the Fair Credit Reporting Act, the Federal Trade Commission (FTC) became responsible for identifying harmed individuals and determining the amount each person would receive. The FTC determined that individual awards would be capped at $1,500 for out-of-pocket expenses and $3,060 for lost time.[46] In both of these examples, the methodologies include a fixed amount of recovery based on the harm individuals are able to demonstrate, incorporating features of both the fixed recovery and individualized determination models.

II. Questions for Public Comment

---

[44] *In Re Dept. of Veterans Affairs Data Theft Litigation*, 1:06-MC-0506-JR (D.D.C. filed January 27, 2009), settlement agreement, pp.9-13.
[45] *United States v. ChoicePoint Inc*., 1:06-CV-0198 (N.D. Ga. Entered February 15, 2006), stipulated final judgment, pp.4, 17.
[46] *See id.* at pp.9-10.

The Department requests comments on the questions below. The Department welcomes comments from all stakeholders, including covered entities and their business associates; State, local, territorial, and tribal governments and their agencies; individuals; and consumer advocates and groups as well as any other interested persons or entities. The Department asks that commenters indicate throughout their submitted comments the question(s) to which a comment is responding.

A. Public Law 116-321

As explained above, Public Law 116-321 amends Part 1 of subtitle D of the HITECH Act to require OCR to consider recognized security practices that organizations adequately demonstrate were in place for the previous 12 months when determining penalties. The Department seeks input from commenters regarding their voluntary implementation of recognized security practices. Additionally, the Department seeks input from commenters on any additional information or clarifications regulated entities need from OCR regarding its implementation of this new law. The first set of questions addresses regulated entities' implementation of "recognized security practices."

1. What recognized security practices have regulated entities implemented? If not currently implemented, what recognized security practices do regulated entities plan to implement?
2. What standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the NIST Act do regulated entities rely on when establishing and implementing recognized security practices?
3. What approaches promulgated under section 405(d) of the Cybersecurity Act of 2015 do regulated entities rely on when establishing and implementing recognized security practices?
4. What other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities do regulated entities rely on when establishing and implementing recognized security practices?

5. What steps do covered entities take to ensure that recognized security practices are "in place"?
    a. What steps do covered entities take to ensure that recognized security practices are in use throughout their enterprise?
        i. What constitutes implementation throughout the enterprise (e.g., servers, workstations, mobile devices, medical devices, apps, application programming interfaces (APIs))?
6. What steps do covered entities take to ensure that recognized security practices are actively and consistently in use continuously over a 12-month period?
7. The Department requests comment on any additional issues or information the Department should consider in developing guidance or a proposed regulation regarding the consideration of recognized security practices.

B. Section 13410(c)(3)

As explained above, Section 13410(c)(3) of the HITECH Act requires the Department to establish a methodology whereby an individual who is harmed by noncompliance with the HIPAA Rules may receive a percentage of a penalty or monetary settlement collected with respect to that noncompliance. Although the Enforcement Rule permits the Department to consider certain types of harm when determining the amount of a penalty, neither the HITECH Act nor the HIPAA Rules define harm generally or for the purpose of identifying and quantifying harm to determine an amount to be shared with an individual. For this reason, the Department seeks input from commenters about how to define harm and what bases should be used for deciding which injuries are compensable.

The first set of questions below addresses what constitutes individual harm in the context of the HIPAA Rules and whether all possible harms or only certain harms should be eligible for a distribution.

8. What constitutes compensable harm with respect to violations of the HIPAA Rules?

a. Should compensable harm be limited to past harm?
    i. Should only economic harm be considered?
    ii. Should harm be limited to the types of harm identified as aggravating factors in assessing CMPs (physical, financial, reputational, and ability to obtain health care)?[47]
    iii. Should harm be expanded to include additional types of noneconomic harms such as emotional harm?
        A. If compensable harm should be expanded to include noneconomic harms, what method should OCR use to evaluate and measure the harm?
b. Should the potential for future harm be compensable?
    i. Are there types of future harm that should not be recognized as compensable? For example, how should OCR treat an individual that has no demonstrated injury-in-fact and only a risk of future harm? What makes future harm likely?
    ii. How will these types of harm be proven and measured?
c. Should OCR allow individuals to include actual and perceived harm, which can vary based upon context and individual, such that different individuals may suffer different amounts of harm even though both suffered the same loss of privacy?
    i. How should such variation in harm be measured?
d. Are there types of harm that should not permit an individual to receive a portion of a CMP or monetary settlement?

9. Should harm be presumed in certain circumstances? For example, should noncompliance with certain provisions of the HIPAA Rules be presumed to have harmed all affected individuals? If so, which provisions?

[47] 45 CFR 160.408(b).

a. Conversely, should noncompliance with certain provisions of the HIPAA Rules be presumed not to have harmed individuals unless some condition is met? For example, should noncompliance with certain workforce training requirements be recognized as harm only when accompanied by an impermissible use or disclosure of PHI?

b. Should the Department require an individual to provide evidence of harm before distributing a portion of a CMP or monetary settlement to that individual? If yes, what types of evidence should be required to demonstrate compensable harm?

10. The Department seeks information about current real-world impacts of loss of privacy on an individual's willingness to seek care or disclose health information to covered entities to better understand the nature of privacy harms that occur.

11. Should the Department recognize as harm the release of information about a person other than the individual who is the subject of the information (*e.g.,* a family member whose information was included in the individual's record as family health history) for purposes of sharing part of a CMP or monetary settlement? If yes, should the individual who is not the subject of the information be permitted to receive a portion of a CMP or monetary settlement?

The HITECH Act gives no direction regarding an amount to be set aside or distributed to individuals other than requiring it to be a percentage of the CMP or monetary settlement. Other federal agencies have approached these determinations in a variety of ways. For example, while the CFPB does not set limits on the amount to be made available for distribution to victims, payments must be practicable.[48] The Securities and Exchange Commission (SEC) exercises discretion regarding whether to apply any or all of a penalty amount to compensate an investor for a loss, with remaining amounts reverting to the US Treasury. The following questions seek comment regarding factors to be considered in establishing a methodology for calculating an

[48] *See* 12 CFR 1075.109 for an explanation of when payments to victims are considered to be "impracticable."

amount to be set aside for distribution to individuals and whether there are circumstances in which funds should not be set aside for distribution.

12. Should there be a minimum total settlement or penalty amount before the Department sets aside funds for distribution?
13. Under Section 13410(c)(3) of the HITECH Act,[49] settlements or CMPs collected in response to a violation of the HIPAA Rules are to be used for the purposes of enforcing the HIPAA Rules. What role should OCR's continued ability to support enforcement activities play in determining whether there should be a minimum total settlement or penalty amount before the Department sets aside funds for distribution?
14. Should there be a minimum amount available per harmed individual before funds are set aside for distribution?
15. Should the Department consider external recoveries or compensation received, available, or likely to be available for harmed individuals when deciding whether to set aside funds for distribution?
16. Should there be a minimum or maximum percentage or amount set aside for distribution? If so, what should the maximum and/or minimum be and why?
17. What factors should the Department consider in determining what total percentage of a CMP or monetary settlement should be set aside for harmed individuals?
    a. For example, should the percentage set aside be dependent upon the number of individuals that may have been harmed, the amount or type of harm, be based on a fixed percentage, or another factor?
    b. Should the percentage set aside take into account OCR's continued ability to support enforcement activities with the remaining funds?

The following questions address how to provide notice to affected individuals that monetary distribution may be available.

---

[49] 42 U.S.C. 17939(c)(3).

18. How should harmed individuals be identified? How should they be notified that they may be eligible for distributions?
19. If an individual is deceased, should the family or estate be notified and eligible to receive a distribution?
20. If an individual cannot be located and notified within the time frame for distribution, should the individual be permitted to receive a distribution at a later date?

The following questions relate to the three recovery models that GAO identified and related considerations regarding the administration of a distribution methodology.

21. What goals should the Department prioritize when selecting a distribution model?
    a. For example, should the methodology ensure that all harmed individuals receive compensation?
    b. Should it instead maximize distributions of available funds to the individuals most harmed by noncompliance?
22. If the Department adopts a model that allows different distributions for differently harmed individuals, how should the distributions be allocated?
23. Should there be a cap on the total percentage amount that any individual can collect to ensure that all harmed individuals receive a distribution or for any other reason?
24. Are there other distribution models to consider? Please provide relevant examples.
25. Should the distribution methodology adjust or deny distribution amounts based on the potential or actual compensation of individuals through other mechanisms outside of the distribution requirement for the same action under the HITECH Act, such as in a manner similar to the CFPB?
26. Should the distribution methodology recognize and account for in-kind benefits (*e.g.,* credit monitoring paid for by the entity) as compensation for purposes of reducing or denying a distribution to those individuals?

27. Should an individual have a right to appeal a decision not to disburse funds to the individual (*e.g.,* where the administrator of the fund determines that the individual did not suffer compensable harm or has received adequate compensation from another source)? If so, how should appeals be adjudicated?
28. Within what timeframe after a settlement agreement or imposition of a CMP should individuals submit claims to be eligible for disbursement?
29. Within what timeframe should funds be disbursed to harmed individuals?
    a. Should timeliness requirements be determined on a case-by-case basis, depending on factors such as the number of individuals affected by a violation?
    b. What other factors should be considered?
30. Finally, the Department requests comment on any additional factors or information the Department should consider in developing a proposed methodology to share a percentage of CMPs and monetary settlements with harmed individuals.

Xavier Becerra,

Secretary,

Department of Health and Human Services.

[FR Doc. 2022-07210 Filed: 4/5/2022 8:45 am; Publication Date: 4/6/2022]